

TeleTrust-Auditorium IT-Sicherheit (it-sa insights) 2026

Nürnberg, 27.10.2026

"Gamechanger in der IT-Sicherheit: Was 2027 technisch, rechtlich, politisch wichtig wird"

Moderation

Prof. Dr. (TU NN) Norbert Pohlmann,

Vorstandsvorsitzender - Bundesverband IT-Sicherheit e.V. (TeleTrust)

Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is)

Westfälische Hochschule, Gelsenkirchen

- Prof. Dr. Norbert Pohlmann zu **"KI-Agenten - mehr als nur ein Buzzword?"**
- RA Karsten U. Bartels LL.M. zu **"Neue IT-Sicherheitsgesetze: Wie Unternehmen schlechte Gesetze in bessere IT-Sicherheit verwandeln"**
- Dr. Kim Nguyen zu **"Deutschland-Stack"**
- Dr. André Kudra zu **"Digitale Souveränität: Was das konsequent bedeutet und was realistisch machbar ist"**
- Diskussion

KI-Agenten - mehr als nur ein Buzzword?

Prof. Dr. (TU NN) Norbert Pohlmann,

Vorstandsvorsitzender - Bundesverband IT-Sicherheit e.V. (TeleTrust)

Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit - if(is)

Westfälische Hochschule, Gelsenkirchen

KI-Agenten als Buzzword

→ Warum plötzlich überall „Agent“ steht

- **Der Begriff „KI-Agent“ weckt Erwartungen**
 - **Mehr Selbstständigkeit**, weniger Handarbeit, **neue Möglichkeiten**.
- **Ein Etikett allein erklärt noch keine Fähigkeit**
 - Was erledigt das System „KI-Agent“ tatsächlich eigenständig?
- **Mehr als ein Buzzword?**
 - Ja, wenn **konkrete Fähigkeiten** einen **sinnvollen Nutzen** schaffen.

KI-Agenten

→ KI mit Autonomie

Ein KI-Agent ist eine **autonome Softwareeinheit**, die auf **Basis von künstlicher Intelligenz eigenständig Entscheidungen trifft** und **Aktionen ausführt, um ein Ziel zu verfolgen**.



■ Ein Agent handelt im Auftrag

- Er **verfolgt ein Ziel** und **entscheidet im erlaubten Rahmen** über **nächste Schritte (Aktionen)**.

■ Auftrag, Grenzen und Befugnisse gehören zusammen

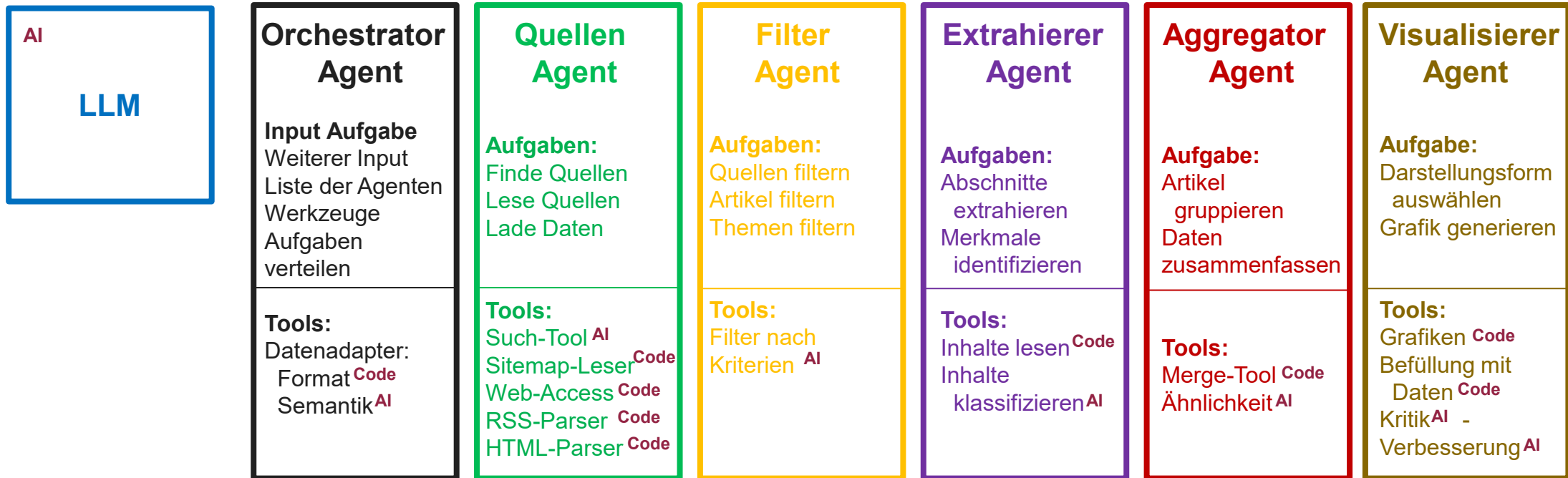
- Wie bei einem menschlichen Beauftragten ist (muss) die Selbstständigkeit begrenzt werden.

- **Wahrnehmung** - *Sammeln / Extraktion* von Daten (User-Interface, Datenbank, **Sensoren** ...)
- **Analyse & Reasoning** - *Bewertung* der Daten, *Schlussfolgerungen* **mithilfe von LLMs**
- **Planung** - *Ziele* definieren, *Aufgaben* priorisieren, in *Teilschritten* aufteilen, **Weg optimieren**
- **Aktionen & Tool-Nutzung** - *zielgerichtete Aktionen ausführen*, *Rechte definieren*, **Tools nutzen**
- **State & Gedächtnis** - *Zwischenergebnisse*, *Historien*, *Präferenzen*, **Aufgaben behalten**
- **Reflexion** - *Eigene Ergebnisse bewerten*, *Pläne* und **Aktionen dynamisch anpassen**
- **Autonomie & Kontrolle** - *temporäre Berechtigungen*, *Sandboxes*, **Protokollierung**

KI-Agenten in der Cyber-Sicherheit

→ Aufgabe für den Marktplatz IT-Sicherheit / if(is)

- **Aufgabe:** Identifikation, Sammlung und Darstellung von IT-Sicherheitstrends im Internet mithilfe **agentischer KI** und deren **Tools**.
- Der **Orchestrator Agent** bekommt die Aufgabe und kann andere Agenten nutzen, um die Aufgabe zu lösen (Multi-Agenten-System).



Herausforderungen von KI-Agenten

→ Handlungsspielräume bewusst gestalten

- **Befugnisse begrenzen**
 - Nur notwendige Datenzugriffe und freigegebene Werkzeuge bereitstellen.
- **Freigaben festlegen**
 - Folgenreiche Aktionen benötigen eine menschliche Entscheidung.
- **Handlungen nachvollziehen**
 - Quellen, Entscheidungen und ausgeführte Schritte protokollieren.
- **Den Betrieb absichern**
 - Mit realistischen Fällen testen, überwachen und bei Problemen stoppen können.



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

KI-Agenten – *mehr als nur ein Buzzword?*

*Ja, wenn Fähigkeiten konkreten Nutzen schaffen.
Chancen nutzen und Handlungsspielräume kontrollieren.*

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen

Vorstandsvorsitzender Bundesverband IT-Sicherheit - TeleTrustT

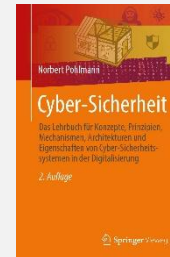
Vorstand im Verband der Internetwirtschaft - eco

if(is)
internet-sicherheit.

Wir empfehlen

Cyber-Sicherheit

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
<https://norbert-pohlmann.com/cyber-sicherheit/>



7. Sinn im Internet (Cyberschutzraum)

<https://www.youtube.com/cyberschutzraum>



Master Internet-Sicherheit

<https://it-sicherheit.de/master-studieren/>



Glossar Cyber-Sicherheit

<https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/>



Vertrauenswürdigkeits-Plattform

<https://www.trust4good.de/>



Besuchen und abonnieren Sie uns :-)

WWW

<https://www.internet-sicherheit.de>

Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

Twitter

https://twitter.com/_ifis

<https://twitter.com/ProfPohlmann>

YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>

www.it-sicherheit.de
Der Marktplatz IT-Sicherheit

Der Marktplatz IT-Sicherheit

Alles rund um IT-Sicherheit: Wissensaustausch, Unterstützung, IT-Sicherheitsanbieter & -Lösungen, News/Artikel/Blogs, Veranstaltungen.

<https://www.it-sicherheit.de/>

Quellen Bildmaterial

Eingebettete Piktogramme: Institut für Internet-Sicherheit – if(is)

- N. Pohlmann, S. Schmidt: „Der Virtuelle IT-Sicherheitsberater – Künstliche Intelligenz (KI) ergänzt statische Anomalien-Erkennung und signaturbasierte Intrusion Detection“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 05/2009
- D. Petersen, N. Pohlmann: "Ideales Internet-Frühwarnsystem", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 02/2011
- M. Fourné, D. Petersen, N. Pohlmann: "Attack-Test and Verification Systems, Steps Towards Verifiable Anomaly Detection". In Proceedings der INFORMATIK 2013 - Informatik angepasst an Mensch, Organisation und Umwelt, Hrsg.: Matthias Horbach, GI, Bonn 2013
- U. Coester, N. Pohlmann: „Verlieren wir schleichend die Kontrolle über unser Handeln? Autonomie hat oberste Priorität“, BI-SPEKTRUM Fachzeitschrift für Business Intelligence und Data Warehousing, 05-2015
- U. Coester, N. Pohlmann: „Ethik und künstliche Intelligenz – Wer macht die Spielregeln für die KI?“, IT & Production – Zeitschrift für erfolgreiche Produktion, TeDo Verlag, 2019
- N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit – Diskussionsgrundlage für den Digitalgipfel 2018“
<https://norbert-pohlmann.com/app/uploads/2018/12/Künstliche-Intelligenz-und-Cybersicherheit-Diskussionsgrundlage-für-den-Digitalgipfel-2018-Prof.-Norbert-Pohlmann.pdf>
- N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit - Unausgegoren aber notwendig“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019
- U. Coester, N. Pohlmann: „Wie können wir der KI vertrauen? - Mechanismus für gute Ergebnisse“, IT & Production – Zeitschrift für erfolgreiche Produktion, Technik-Dokumentations-Verlag, Ausgabe 2020/21
- D. Adler, N. Demir, N. Pohlmann: „Angriffe auf die Künstliche Intelligenz – Bedrohungen und Schutzmaßnahmen“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2023
- P. Farwick, Pohlmann: „Chancen und Risiken von ChatGPT – Vom angemessenen Umgang mit künstlicher Sprachintelligenz“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 4/2023
- N. Pohlmann: Lehrbuch „Cyber-Sicherheit“, Springer Vieweg Verlag, Wiesbaden 2022
Druckausgabe (ISBN 978-3-658-36242-3) und eBook (ISBN 978-3-658-36243-0).

Weitere Artikel siehe: <https://norbert-pohlmann.com/artikel/>

Neue IT-Sicherheitsgesetze: Wie Unternehmen schlechte Gesetze in bessere IT-Sicherheit verwandeln

Rechtsanwalt Karsten U. Bartels LL.M.,
Stellvertretender Vorstandsvorsitzender - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Leiter TeleTrusT-AG "IT-Sicherheitsrecht"
HK2 Rechtsanwälte

Gesetze in bessere IT-Sicherheit verwandeln

IT-Sicherheitsgesetze sind ...

- nicht/ wenig aufeinander abgestimmt
- Ergebnis einer politischen Einigung und keine fachliche Bestleistung
- Mehrfachregulierung

- relativ unbürokratisch
- weitgehend offen hinsichtlich der konkreten Umsetzung
- überfällig.

DSGVO

Cyber Resilience Act

Geschäftsgeheimnisschutz-
Gesetz

Produkthaftungsgesetz

KI-Verordnung

Bereichsspezifische
IT-Sicherheitsgesetze

NIS-2-Umsetzungsgesetz
+ KRITIS-Dachgesetz

Gesetze in bessere IT-Sicherheit verwandeln

Umsetzung durch ...

- Orientierung an Risiken
- Priorisierung und Orientierung an Ressourcen
- Gemeinsamkeiten vor die Klammer ziehen
 - Maßnahmen nach dem Stand der Technik
 - Dokumentation
 - Lieferkettenmanagement
 - IT-Sicherheitsvereinbarungen nutzen
- Multi-Domain-Teams (inklusive Recht)
- vorausschauendes Legal Monitoring.

Deutschland-Stack

Dr. Kim Nguyen,
Vorstandsbeisitz - Bundesverband IT-Sicherheit e.V. (TeleTrusT),
Leiter TeleTrusT-AG "Cyber-Nation"
Bundesdruckerei

DEUTSCHLAND-STACK

Ein digitales Fundament. Gemeinsame Verantwortung.

Was gehört dazu?

Technologische Basis, Rahmen und Produkte

Wo stehen wir?

Verbindliche Standards in sieben Technologiefeldern

Was ist noch offen?

Betrieb, Governance und Konformitätsmodell



TELETRUST

Sicherheit als Architekturprinzip

Ein verbindliches Gesamtmodell für Architektur, Governance und Betrieb

KI generiert

EUROPÄISCH
ANSCHLUSSFÄHIG

BUND



SICHER
SOVERÄN
VERTRAUENSWÜRDIG

6 ANWENDUNGEN & DIENSTE

5 BASISDIENSTE

4 PLATTFORM

3 ENTWICKLUNG, SICHERHEIT & BETRIEB

2 INFRASTRUKTUR

BETRIEB

HOCHSICHERHEIT

ARCHITEKTUR

Vom Katalog zur Zielarchitektur

Referenzen, Schnittstellen und Anwendungsfälle.

Souveränität im Betrieb

Kontrolle, Resilienz und Wiederanlauf.

Durchgängig verankert

Identität, Kryptografie und Lebenszyklus.

Nicht die Zahl der Bausteine, sondern ihre Beherrschbarkeit entscheidet.

LÄNDER

KOMMUNEN

RESILIENT
VERFÜGBAR
ZUKUNFTSFÄHIG

DREI ARBEITSGRUPPEN

Drei Perspektiven. Eine sichere Zielarchitektur.

TeleTrust übersetzt die Position in konkrete Anforderungen und Modelle.

KI generiert



01 HOCHSICHERHEIT

Schutz für kritische Szenarien

Zero Trust · Identitäten · Kryptografie ·
Wiederanlauf

02 INFRASTRUKTUR & BETRIEB

Resilienz wird im Betrieb bewiesen

ISMS · SOC · DevSecOps · Backup · Härtung

03 GOVERNANCE

Verantwortung wird verbindlich

Rollen · Konformität · Beschaffung · Auditierung

Referenzarchitektur, Betriebsmodell und Governance greifen als ein System ineinander.

Digitale Souveränität: Was das konsequent bedeutet und was realistisch machbar ist

Dr. André Kudra,

Vorstandsbeisitz - Bundesverband IT-Sicherheit e.V. (TeleTrusT),
CIO esatus AG

Konsequent heißt: vollständige EU-Kontrolle

SEAL-4: VOLLE DIGITALE SOUVERÄNITÄT

Unabhängige und selbstbestimmte Nutzung digitaler Funktionen und Dienste

Höchste Stufe im Cloud Sovereignty Framework der EU-Kommission (Oktober 2025)

1

Recht

Nur europäisches Recht gilt. Fremde Gesetze mit grenzüberschreitender Reichweite, etwa der US CLOUD Act, greifen nicht.

2

Technik und Betrieb

Europäische Akteure betreiben, unterstützen und entwickeln den Dienst, ohne Anbieter von außerhalb der EU.

3

Lieferkette

Auch Hardware, Firmware und Software stammen nicht aus kritischen Abhängigkeiten außerhalb der EU.

Acht Ziele, unterschiedlich gewichtet

Ziel		Leitfrage	Gewicht im Score	
SOV-1	Strategie	Wer besitzt und steuert den Anbieter?	<div></div>	15%
SOV-2	Recht	Welches Recht reicht in den Dienst hinein?	<div></div>	10%
SOV-3	Daten und KI	Wer kontrolliert die krypto. Schlüssel, Zugriff und Standort?	<div></div>	10%
SOV-4	Betrieb	Kann Europa den Dienst allein betreiben?	<div></div>	15%
SOV-5	Lieferkette	Woher kommen Hardware, Firmware und Software?	<div></div>	20%
SOV-6	Technologie	Offen, auditierbar und ohne Lock-in?	<div></div>	15%
SOV-7	Sicherheit	Wer betreibt Security und führt Audits durch?	<div></div>	10%
SOV-8	Umwelt	Energie, Kreislauf und Rohstoffe auf Dauer?	<div></div>	5%

Quelle: Europäische Kommission, Cloud Sovereignty Framework (Oktober 2025).

Die Skala: fünf Stufen, der schwächste Punkt zählt

SEAL-0
Keine Souveränität
Kontrolle und Recht
liegen vollständig
außerhalb der EU.

SEAL-1
Jurisdiktion
EU-Recht gilt formal, ist
aber kaum
durchsetzbar.

SEAL-2
Daten
EU-Recht gilt,
wesentliche
Abhängigkeiten bleiben.

SEAL-3
Technologie
EU-Akteure haben
bedeutenden Einfluss,
Dritte nur marginal.

SEAL-4
Volle Souveränität
Vollständige EU-
Kontrolle, keine
kritischen
Abhängigkeiten.

**Das Gesamtniveau ist das niedrigste Niveau über alle acht Ziele.
Ein schwacher Punkt zieht alles nach unten.**

SEAL-4 ist kaum erreichbar



Hardware und Chips

Solange Chips und Hardware von außerhalb der EU abhängen, ist SEAL-4 kaum erreichbar.
Die Kommission sieht das selbst so.



Die Prüfung ist umfassend und aufwendig

Geprüft wird die ganze Kette bis zu den Lieferanten, meist auf Basis von Selbstauskünften.
Einheitliche Fragen und Nachweise sollen helfen.



Mindestniveau statt Maximalanspruch

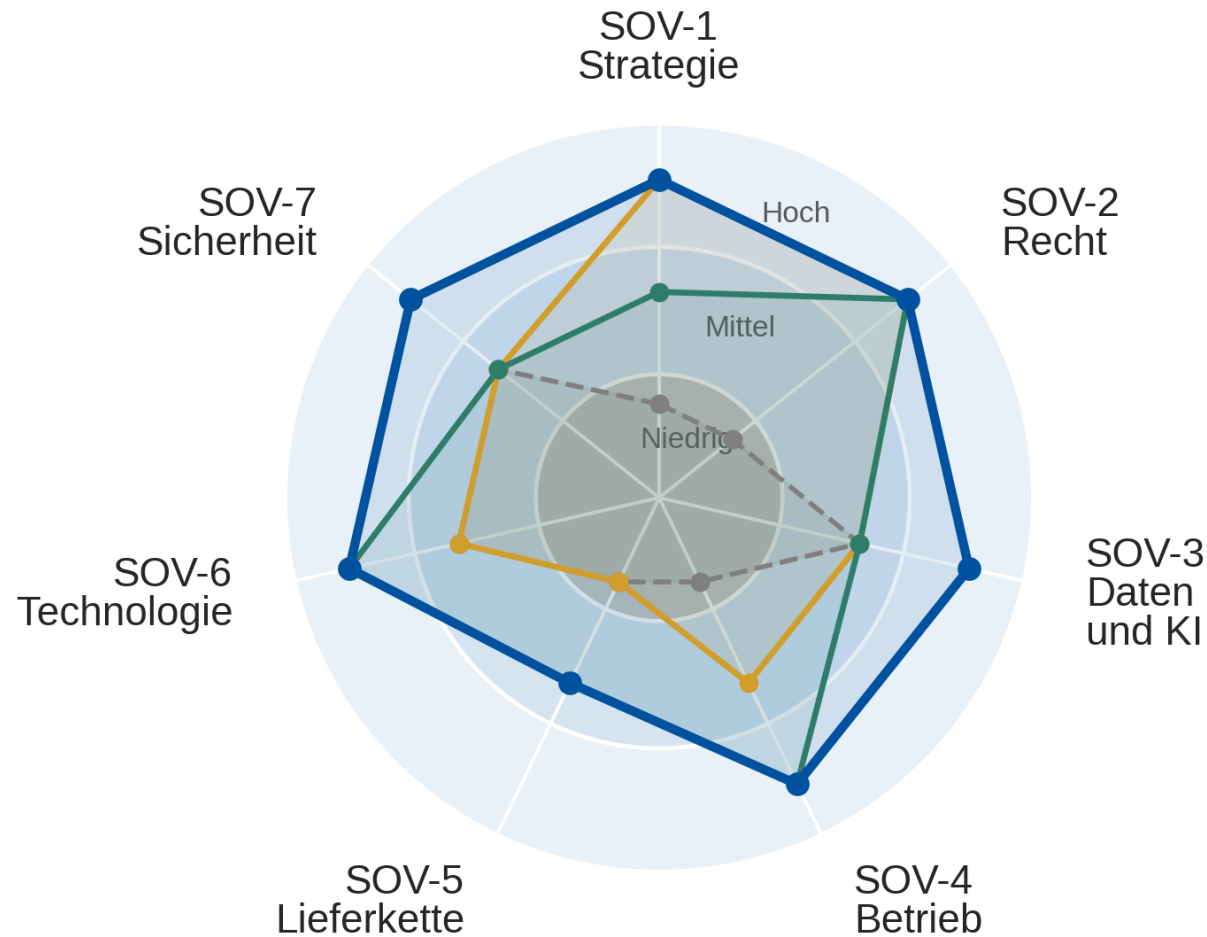
Ein Mindestniveau je Anwendung macht Anbieter vergleichbar.
Die Forderung nach SEAL-4 für alles tut das nicht.

Vier Betriebsmodelle gegen acht Ziele

		Globaler Hyperscaler	EU Hyperscaler	Open Source in DE	Dedizierte Lösung
SOV-1	Strategie	Niedrig	Hoch	Mittel	Hoch
SOV-2	Recht	Niedrig	Hoch	Hoch	Hoch
SOV-3	Daten und KI	Mittel	Mittel	Mittel	Hoch
SOV-4	Betrieb	Niedrig	Mittel	Hoch	Hoch
SOV-5	Lieferkette	Niedrig	Niedrig	Mittel	Mittel
SOV-6	Technologie	Mittel	Mittel	Hoch	Hoch
SOV-7	Sicherheit	Mittel	Mittel	Mittel	Hoch
SOV-8	Umwelt	Hängt vom Anbieter ab	Hängt vom Anbieter ab	Hängt vom Anbieter ab	Hängt vom Anbieter ab

Eigene Einschätzung zur Diskussion. Die Einstufung ist nicht Teil des Frameworks.

Die Profile im Überblick



Globaler Hyperscaler

EU-Hyperscaler

Open Source in DE

Dedizierte Lösung

Recht

Alle europäischen Modelle liegen vorn. Die Strategie hängt vom Eigentümer ab.

Daten und KI

Hohe Schlüsselhoheit gibt es nur bei der dedizierten Lösung.

Lieferkette

Kein Modell kommt über Mittel hinaus. Hardware und Chips bleiben die Hürde.

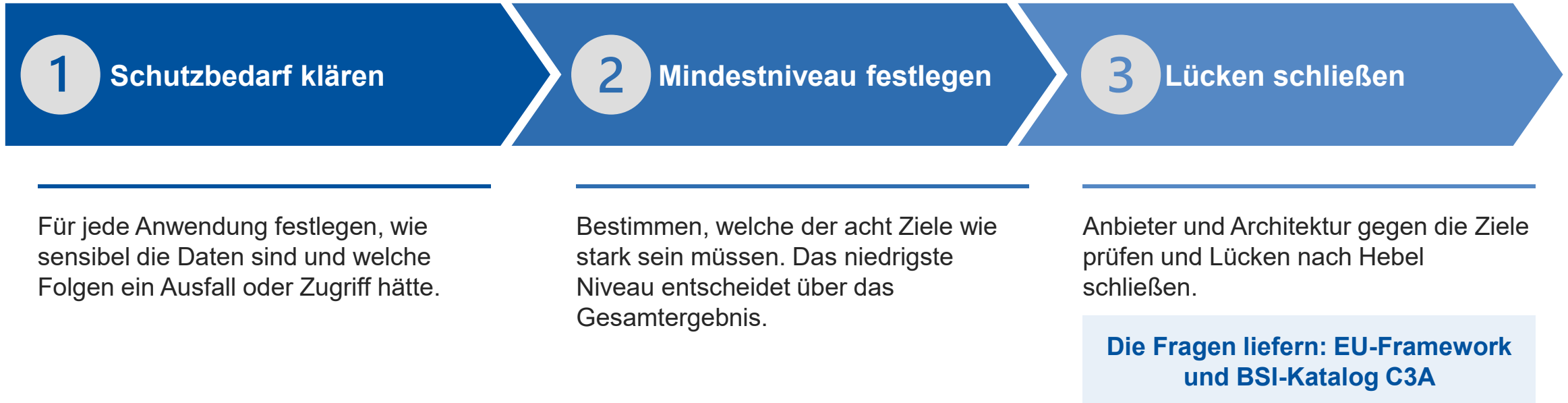
Eigene Darstellung. SOV-8 Umwelt ist nicht modellabhängig und fehlt hier. Grafik generiert mit Claude.

Je sensibler, desto höher das Mindestniveau

Anwendung	Schutzbedarf	Mindestniveau					Worauf es ankommt
Büro-Kollaboration, interne Dokumente	normal	Seal-1 bis 2					Wechseln können, ohne Lock-in → Betrieb, Offene Standards
		0	1	2	3	4	
Fachverfahren mit personenbezogenen Daten	hoch	Seal-2 bis 3					EU-Recht, Kontrolle über die Daten, sicherer Betrieb → Recht, Daten, Sicherheit
		0	1	2	3	4	
Schlüsselmaterial und Identitäten	Sehr hoch	Seal-3 bis 4					Schlüssel, Eigentümer und Lieferkette in EU-Hand → Schlüsselhoheit, Strategie, Lieferkette
		0	1	2	3	4	

Nicht überall SEAL-4, sondern je Anwendung das Niveau, das der Schutzbedarf verlangt.

Vorgehen in 3 Schritten



Der erste Schritt ist am Montag machbar: Schutzbedarf der wichtigsten Anwendungen klären.

Konsequent

SEAL-4

Vollständige EU-Kontrolle über alle acht Ziele. Ein Maßstab, kein Normalfall.

Realistisch

SEAL-2

Ein Mindestniveau: Die EU selbst setzte für ihre Ausschreibung SEAL-2 als Minimum.

Der Schwächste zählt

Lieferkette

Ein schwacher Punkt zieht alles nach unten. Lieferkette und Hardware bleiben für alle Modelle die Hürde.

Danke.

Fragen und Diskussion



Dr. Andre Kudra

CIO, esatus AG
Vorstandsbeisitzer
TeleTrust

a.kudra@esatus.com

Diskussion und Fragen?